COMP-649B 2009 Homework set #2

Due Tuesday March, 3 2009 in class

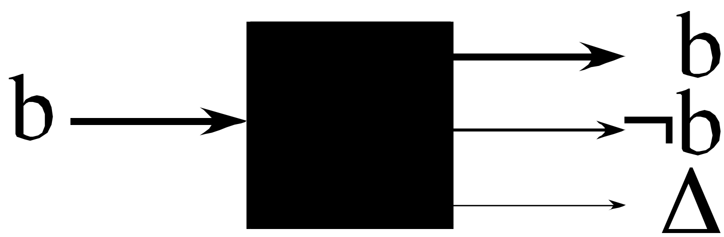
A. BB84 vs Projective Measurements

[15%] Prove that every projective measurement Eve may perform on the BB84 transmissions will induce an error probability $\geq 25\%$ and that the least error probability is reached by resending the exact same state she has observed.

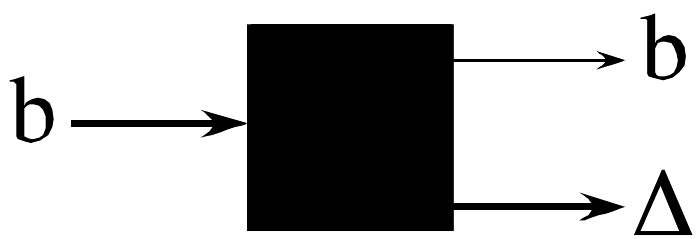
B. B92 vs distinguishing $|0\rangle$ from $(|0\rangle+|1\rangle)/\sqrt{2}$

Construct two generalized measurements such that using $|\psi_0\rangle=|0\rangle$ or $|\psi_1\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$ we get

[10%] **1)** on input $|\psi_b\rangle$ an output $b\in\{0,1\}$ with probability $\alpha=2-\sqrt{2}\approx 59\%$, an output $\neg b$ with probability $\alpha/2\approx 29\%$, and an erasure Δ with the remaining probability $1-3\alpha/2\approx 12\%$.



[10%] **2)** on input $|\psi_b\rangle$ an output $b\in\{0,1\}$ with probability $\alpha/2\approx 29\%$, and an erasure Δ with the remaining probability $1-\alpha/2\approx 71\%$. (notice that this measurement never answers $\neg b$)



Now consider these two measurements as channels.

[10%] **3)** Define the projective measurement $\{|\phi_0\rangle,|\phi_1\rangle\}$ with symmetric probabilities

$$\Pr[\text{output}=|\phi_0\rangle \mid \text{input}=|\psi_1\rangle) = \Pr[\text{output}=|\phi_1\rangle \mid \text{input}=|\psi_0\rangle) \text{ and}$$
$$\Pr[\text{output}=|\phi_0\rangle \mid \text{input}=|\psi_0\rangle) = \Pr[\text{output}=|\phi_1\rangle \mid \text{input}=|\psi_1\rangle)$$

What performances do you obtain by measuring this complete measurement ?

[10%] **4)** Which of the three is most resistant to privacy amplification ? Explain.

[10%] **5)** What can you say regarding question **A.** above with respect to the B92 scheme instead of the BB84 scheme. How does this relate to questions **1)** and **2)** above ??

…more on back

C. <u>BB84 conjugate bases</u>

The rectilinear RL={ $|0\rangle$, $|1\rangle$ } and diagonal DG= $\{ (|0\rangle+|1\rangle)/\sqrt{2} , (|0\rangle-|1\rangle)/\sqrt{2} \}$ bases are called *conjugate* because the states of any one basis measured in the other will produce completely random outcomes.

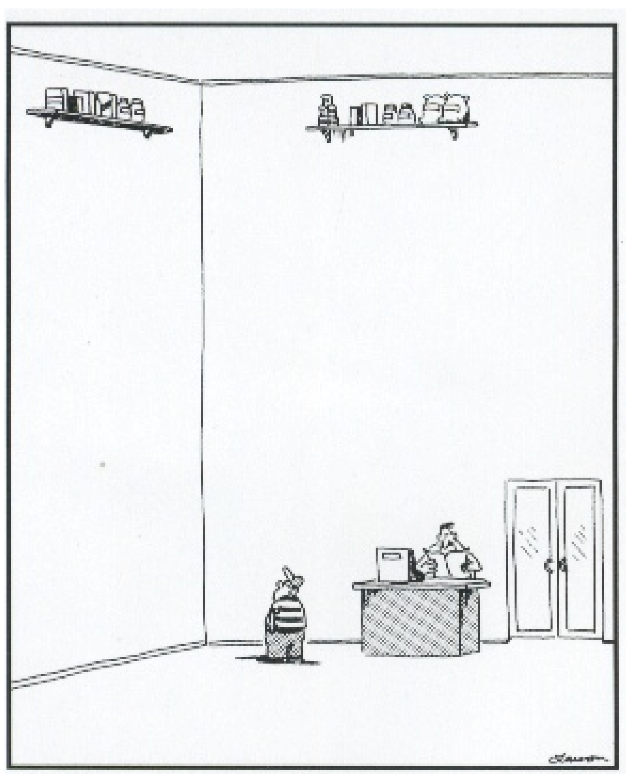
[10%] Show that there exists yet a third basis CI of a single qubit that is conjugate to both RL and DG.

[10%] Show there is not a fourth such basis.

D. <u>Sampling</u>

Suppose that Alice has a random n-bit string X_A and that Bob has an n-bit string X_B erroneous in t positions (with respect to X_A) and correct in n-t positions. Now imagine they pick at random n/2 positions from 1 to n and compare the corresponding bits. Let m be the number of errors observed out of n/2 positions. Let $\mu=2m/n$ be the observed average.

[15%] Show that the probability that the remaining n/2 positions contain more than $(\mu+\delta)$ n/2 errors decreases exponentially fast for $\delta>0$.



Inconvenience stores

…more on back